Something in the air:

WEP2, credibility zero

Thom Stark (thom@starkrealities.com)
Professional curmudgeon
September 2001

> The shortcomings of WEP (Wireless Equivalent Protocol) are legion. That's why there's been so much pressure on the IEEE to get WEP2 out the door. The problem is, WEP2 doesn't really fix anything.

Last year, while we were house hunting and getting prepared to move and I had a zillion things on my plate all at the same time, one of my neighbors in El Cerrito, where we used to live, stopped me on the street to ask for my assistance.

I thought about the meeting I was scheduled to attend and the dozen other tasks that I'd have to wade through before day's end and I made an executive decision to blow him off.

"I'm awfully busy," I replied. "Can it wait until tomorrow afternoon? I'll have a lot more time then."

"No," he said, "I don't think so."

Then he showed me why and I had to admit that he was right. It really couldn't wait.

My neighbor was a contractor, you see, and somehow he'd managed to rip a flap of skin about the size of a poker chip off the ball of his left thumb. It was still attached along one edge, but the flesh underneath was raw and oozing and my neighbor -- a southpaw -- was fully occupied just keeping pressure on it to staunch the bleeding.

So I invited him in, washed off his wound, doused it with peroxide, cut off the dangling skin, smeared Bacitracin on it, and taped a bulky gauze compress over it to keep it clean.

"You'll have to change that dressing at least once a day to abate infection," I told him.

"Can't I just put a Band-Aid on it?" he asked.

"No," I responded, shaking my head, "this requires serious medicine. A Band-Aid just isn't enough."

That's the thing about Band-Aids. They're just the ticket for little nicks and scrapes, but when the injury is at all major, they're an inappropriate treatment. Messing around with Band-Aids in that circumstance accomplishes nothing useful -- and it gets in the way of more suitable therapy.

Whistling in the dark

As Larry Loeb documented here on *developerWorks* back in April, 2001 the Wired Equivalent Protocol upon which 802.11b WLANs depend for encryption, authentication, and repudiation of data is riddled with fundamental architectural flaws. The initialization vector (IV) that's generated every time a Wi-Fi NIC powers up is a maximum of just 24 bits long, and some cards simply give it an initial value of 0, and then

Contents:

Whistling in the dark
We're going wrong
I want a new drug
Bring it on home
Resources
About the author
Rate this article

Related content:

What's up with WEP?
Shut the door! They're coming in the windows!
More dW Wireless resources
Subscribe to the developerWorks newsletter

Also in the Wireless zone:

Tutorials
Tools and products
Articles

increment that value by 1 every time they send or receive a packet.

To make matters worse, the IV used to generate the cipher is transmitted along with every packet. That's pretty lame and it makes the RC4 stream cipher WEP uses for payload encryption extremely vulnerable to reuse exploits -- especially since, 9 times out of 10, the "secret" key that is used together with the IV to encrypt the data is merely the Service Set Identifier (SSID) of the network (and is also, therefore, identical for every user on that 'net).

As if that weren't bad enough, Scott Fluhrer of Cisco Systems, and Adi Shamir and Itsik Mantin of the Eizer Weizmann Institute described a brand-new attack to recover encrypted passwords from the RC4 cypher in a joint paper they presented at the Selected Areas in Cryptography (SAC) conference in Toronto just this August. Adam Stubblefield of Rice University, and John Ioannidis and Aviel D. Rubin of AT&T Labs hammered the final nail into WEP's coffin when they implemented that very attack against a 128-bit WEP secret key -- and did it a week before the SAC conference opened, using only off-the-shelf hardware and an exploit program, the original version of which took them only hours to write.

There are similarly major problems with every aspect of WEP, from CRC32 calculation to key management, and every one of them is exploitable. Merely beefing up the IV to 128 bits won't close the gaping security holes in WEP, either. That's the equivalent of putting a Band-Aid on a sucking chest wound. It might look good to an untrained observer, but it doesn't stop the hemorrhage.

None of this is exactly a top secret.

We're going wrong

Unfortunately, the TGI Working Group of the IEEE -- the body that developed WEP -- has adopted a palliative strategy comparable to wrapping a Band-Aid around the most freely bleeding injuries of the current version. They're calling the result WEP2.

As Rocket J. Squirrel of Rocky & Bullwinkle fame was wont to say, "That trick never works."

In May, 2001, Bernard Aboba of Microsoft presented an analysis of the security holes in the original recipe of WEP as a point of departure from which to examine how the extra-crispy version of WEP2 addresses them. Without going into a great deal of detail, his slides bullet-point his findings pretty succinctly:

- WEP2 does increase the IV key space to 128 bits, but it fails to prevent IV replay exploits and still permits IV key reuse.
- That same IV replay weakness, combined with a faked MAC address, also permits an attacker to forge authentication.
- Known plaintext exploits -- where the intruder knows or can guess part or all of the data payload or encrypted header contents and uses that information, plus the IV key and CRC32 to crack the encryption itself -- work as well with WEP2 as they did with WEP1.
- The inclusion of mandatory KerberosV support merely opens WEP2 to new dictionary-based attacks. (Aboba estimates that up to 10% of Kerberos-"protected" user passwords can be cracked within 24 hours, using an inexpensive network of PCs running parallel DES cracking techniques.)
- Because reassociate and disassociate messages are not secure, WEP2 is vulnerable to DoS attacks similar in nature to the syn-flood techniques that bedeviled Amazon.com last year.
- Because beacon messages are not authenticated, client nodes can roam to a rogue AP, which could completely compromise them.

According to Aboba, the only good news is that real-time decryption of WEP2 data streams -- necessary to eavesdropping on data exchanges as they take place -- will be significantly more difficult, due to the increased size of the IV key space.

I want a new drug

The fundamental problem from which these vulnerabilities all derive is that WEP2 is being designed to be downwardly compatible with and to interoperate with WEP1. Many engineers think that's a major architectural blunder, because WEP1 simply wasn't designed for security from the ground up, and to meet the IEEE's goal of interoperability, WEP2 will have to be built on that same, insecure foundation.

In my book, the right answer is to pull the plug on WEP altogether and to replace it with a protocol that is

designed from its inception to be truly secure.

I'm far from the only one who thinks that way. In fact, at the 2001 meeting of the IEEE's P802.11 full working group in Orlando, FL -- the meeting where Aboba presented his analysis of the protocol's many vulnerabilities -- a motion to remove WEP2 from the next draft of the 802.11 spec failed by a very close vote of 30 to 36 with one abstention.

When 45% of those responsible for approving WEP2 want to make it go away, I think it's safe to say that it has fallen a good deal short of an overwhelming mandate for adoption, even among those who have a vested interest in it.

The principal remaining roadblock to just throwing WEP2 out and starting over appears to have been a strong reluctance on the part of many of the IEEE folks to "waste" the effort they've invested thus far. Just over half of those who voted apparently think the problems with WEP and its offspring can be fixed; that the work they've done can be salvaged.

Luckily, at the same meeting, the TGI folks also voted to call for new authentication proposals, which leaves open the door to continued debate about the subject of WEP's successor.

In the short term, the IEEE folks may just settle for replacing that grungy old WEP Band-Aid with a new, stickier WEP2 Band-Aid. Eventually, however, they're going to have to deal with the underlying malady.

Bring it on home
WEP is broken. It can't be fixed, because its problems are too integral a consequence of its core design.

It needs to be replaced with something fundamentally different; something that is designed from the ground up to provide robust key generation and management, sturdy bulk encryption, authentication and data integrity mechanisms, and a high degree of transparency for the end user.

If that new security protocol is turned off by default, though, up to half of all users won't turn it on. And, if it isn't dead easy to configure and maintain, some "admins" will always turn it off.

I've walked among them and I know. There are many secretaries, clerks, and other lower-level employees who have become the office admin by virtue of having been the one to unbox the AP. Almost invariably, they get no special recognition or extra pay for their admin duties. In fact, their performance reviews rarely even accommodate the demands that running a network makes on their time, much less acknowledging them for the time they spend administering one.

They're the target audience for WEP's true successor. It must be designed to protect those admins and their users from bad guys, in spite of their own lack of expertise, interest, and/or concern about intruders. And it must do a good job of it, without interfering with them or their users.

And no more Band-Aids, please. Wireless security requires serious medicine.

Next time: Peter Shipley coined the term 'war-driving' to describe his survey of open WLANs in the San Francisco Bay Area. What he has discovered is shocking, compelling, and downright scary.

Resources

- See the Stubblefield/Ioannidis/Rubin paper on their implementation of the Fluhrer/Mantin/Shamir theoretical attack (in PostScript format).
- See the *developerWorks* article, "What's up with WEP?"
- See this HTML summary of the security shortcomings of WEP, including a link to the full draft report.
- Review Bernard Aboba's analysis of WEP2 security.
- IBM scientists Bruce Rich, Anthony Nadalin, and Theodore Shrader present a primer on KerberosV.
- Read Thomas Wu's 1998 article entitled "A Real-World Analysis of Kerberos Password Security".
- See John Gilmore's DES Cracker Project.
- Review the Tentative minutes of IEEE 802.11 full working group's 2001 meeting (see section 27 for the vote to remove WEP2 from the spec).

- See the last installment in this column by Thom Stark entitled "Shut the door! They're coming in the windows!"
- Return to the developerWorks Wireless topic for more Wireless resources.

About the author

Thom Stark is a professional writer and an amateur horseman. He lives in Mariposa, California, home of Yosemite National Park. He owns several acres of oak trees and gopher holes, and has a wife, a dog, and a decrepit Mercedes convertible, all of which he loves. He makes his living by advocating common sense and a focus on delivering value to end users. His hobbies include reading comics and science fiction, playing the guitar and singing -- occasionally on key. His passions include the life of Alexander the Great, and leaving the world a better place than he found it. He also writes a monthly column and occasional feature articles for Boardwatch Magazine. He maintains a non-commercial Web site (http://www.starkrealities.com) where much of his work is archived.